



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/928,983	08/13/2001	Barry J. Gilhuly	1400-1072P6	8317
47243	7590	04/05/2006	EXAMINER	
DANAMRAJ & YOUST, P.C. PREMIER PLACE, SUITE 1450 5910 NORTH CENTRAL EXPRESSWAY DALLAS, TX 75206			REILLY, SEAN M	
			ART UNIT	PAPER NUMBER
			2153	

DATE MAILED: 04/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/928,983	Applicant(s) GILHULY ET AL.	
	Examiner Sean Reilly	Art Unit 2153	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 January 2006.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 17-20 and 105-174 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 17-20 and 105-174 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This Office action is in response to Applicant's amendment and request for reconsideration filed on January 19, 2006. Claims 17-20 and 105-174 are presented for further examination. All independent claims have been amended.

Double Patenting

All double patenting rejections have been withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

- 1. Claims 17-18 and 105-139 are rejected under 35 U.S.C. 103(a) as being unpatentable over AirMobile Communication Server Guide ("AirMobile Software for Lotus cc:Mail Wireless," Motorola Publication, 1995, hereinafter "AirMobile"), in view of Doonan et al. (U.S. Patent No. 6,807,277, hereinafter "Doonan") and Gehrmann et al. (International Publication No. WO 00/31931).**

In considering claims 17 and 111, AirMobile discloses the claimed redirection method including detecting a new data item for the user at the messaging host system (cc:Mail Post Office server, Fig. 1), forwarding a copy of the data item to a redirector host system (AirMobile Wireless for cc:Mail Server, Fig. 1), determining if the new data item should be redirected from

Art Unit: 2153

the redirector host system to the user's mobile device, and if so, then packaging the data item in an electronic envelope and transmitting the electronic envelope to the user's mobile device (pp. 10-11, describing the messaging system and the filtering of messages at the redirector host system, see also pp. 25-26, 35).

AirMobile further discloses that messages are sent in a "secure and authenticated" manner between the LAN-based server and the mobile wireless device – see p. 25. However, AirMobile does not explicitly state that the secure manner includes encryption. Nonetheless, encryption is a notoriously well-known device used to create secure channels between communicating systems, as evidenced by Doonan. In an analogous messaging system, Doonan discloses a system where messages are sent from a server (Col 3, lines 28-32) to a recipient, wherein the messages are encrypted at the server using a key generated at a key server and obtained from the key server (Col 2, lines 1-18). The encrypted message is then sent to the recipient device that in turn decrypts the message using a decryption key obtained from the key server (Col 2, lines 1-18). The keys passed from the key server to the sender and receiver are sent over a secure communications link (secure HTTP, Col 3, line 42). Given this teaching, a person having ordinary skill in the art would have readily recognized the desirability and advantages of using encryption, as disclosed by Doonan, at the mail server, in the system taught by AirMobile to securely transmit messages, because encryption is a very effective way to ensure that messages remain secure throughout their transmission. Therefore, it would have been obvious to encrypt the messages at the AirMobile Wireless for cc:Mail Server in the system taught by AirMobile.

AirMobile and Doonan disclosed the invention substantially as claimed however, AirMobile and Doonan both failed to specifically recite using the redirector host system to automatically encrypt data items. Nonetheless it was widely known in the art at the time of the invention to automatically encrypt data items at redirection servers, as evidenced by Gehrman. In an analogous messaging system Gehrman disclosed a system for redirecting messages from a mail server to user's wireless device (see inter alia Figure 1 and pg 5, lines 12-21; forwarding message from the mail server 24 to the client PC or PDA over wireless connection 20). Further when Gehrman's system determines that a new data item should be redirected (i.e. "meeting the user's predetermined mail forwarding policy) the system automatically encrypts the data item before redirecting it to the client's PDA (see inter alia pg 8, line 29 – pg 9, line 9). Gehrman's system employs this automatic encryption scheme to ensure that unencrypted messages that are going to be sent over unsecured communication networks are first encrypted to ensure messages remain secure throughout their transmission (pg 3, lines 13-26). Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the automatic encryption scheme used by Gehrman's in the combined AirMobile and Doonan system to ensure messages remain secure throughout their transmission (pg 3, lines 13-26).

In considering claim 18, neither AirMobile nor Doonan disclosed sending the decryption key to the mobile device over a serial connection between the computer system and the mobile device. Nonetheless, Doonan disclosed that the encryption keys can be passed any number of ways (Col 3, lines 40-45). Further it was widely known at the time of the invention to use serial connections for communication between two devices. Thus, it would have been obvious to one

Art Unit: 2153

of ordinary skill in the art at the time of the invention to send the encryption keys using a serial communication, since serial communication protocols are widely used and further are a cheap means for communication.

Claims 105-107 are disclosed on page 10 of AirMobile.

In considering claims 108-109, AirMobile further discloses the step of configuring filtering rules and a user profile database at the redirector host system and allowing a user or administrator to remotely configure the filters and database remotely (pp. 11-12).

Claims 110 are further disclosed by the combination of AirMobile and Liao (see AirMobile, pp. 26-27).

In considering claim 10, Liao further discloses that the encryption includes using a cipher algorithm and a decryption key to decrypt the encrypted new data item (col. 7, lines 18-20, 60-61; col. 9, lines 4-9).

In considering claim 11, Liao further discloses generating the decryption key at the redirector host system and forwarding the key to the mobile device using a secure communications link (col. 9, lines 22-52).

Claims 13-14, and 21 are further disclosed by Liao (see cols. 7-10, describing in depth the process of sending keys between the mobile device and host to enable encryption and decryption between the two devices).

In considering claim 113, AirMobile further discloses sending replies from the mobile device to the redirector host system (p. 26, describing messages sent by the mobile device). Thus, given the teaching of Liao, it would have been obvious to include encryption and decryption of these messages from the mobile device to the host in the same way as the initial messages sent from the host to the mobile device, in order to enable two-way secure transactions.

In considering claim 114, the messages sent from the mobile device to the redirector server will necessarily be addressed using the address of the redirector host system.

Claims 115-116 disclose the analogous reverse steps as claim 1, and thus are rejected under the same rationale as claim 1.

In considering claim 117, the combined system of AirMobile and Doonan, as described above, will necessarily complete the claimed steps of decrypting the encrypted reply received at the redirector host system, reconfiguring address information associated with the reply, and sending the reconfigured reply data to a destination using an electronic address included in the reply data item (i.e. the messages sent from the mobile device are intended for outside recipients,

so must include the address of those recipients and must have addresses reconfigured upon redirection at the redirection host system).

In considering claim 118, AirMobile and Doonan both further disclose the claimed gateway, and thus sending messages in the electronic envelope through the gateway (AirMobile, Fig. 1, wherein the "Mobidem" serves as the gateway; Liao, Fig. 1, wherein the "up.link gateway" is the gateway).

Claims 119-128 are disclosed in the same sections of AirMobile discussed previously.

In considering claims 129-132, neither AirMobile nor Doonan disclose that the e-mail server is part of an ISP. Nonetheless, Examiner takes Official notice that it is well known for ISPs to run e-mail servers. Thus, it would have been obvious for the e-mail systems taught by AirMobile and Liao to be run by an ISP because that would increase business with the ISP.

In considering claim 133, AirMobile further discloses that the redirector host system includes a further messaging host system (Fig. 1, cc:Mail PostOffice; cc:Mail router).

In considering claim 134, AirMobile further discloses that the redirector host system in incorporated with the messaging host system (Fig. 1, all host systems are cc:Mail).

In considering claims 135 and 136, Doonan further discloses that the host system can be a Web server, which would include web-page interfaces. Thus, it would have been obvious to use a web-based interface to control the filtering in the AirMobile system because such an interface is ubiquitous and could be used anywhere in the world.

Claims 137-138 are further disclosed by the sections of AirMobile previously discussed.

In considering claim 50, Examiner takes Official notice that compression of electronic messages is well known. Thus, it would have been obvious to compress the messages being sent from the redirector host system to the mobile device to conserve network bandwidth.

2. **Claims 19-20, 140-146 and 148-174 are rejected under 35 U.S.C. 103(a) as being unpatentable over AirMobile Communication Server Guide ("AirMobile Software for Lotus cc:Mail Wireless," Motorola Publication, 1995, hereinafter "AirMobile"), in view of Liu et al. (U.S. Patent No. 6,760,752, hereinafter "Liu") and Gehrmann et al. (International Publication No. WO 00/31931).**

In considering claims 19 and 20, AirMobile discloses the claimed redirection method including detecting a new data item for the user at the messaging host system (cc:Mail Post Office server, Fig. 1), forwarding a copy of the data item to a redirector host system (AirMobile Wireless for cc:Mail Server, Fig. 1), determining if the new data item should be redirected from the redirector host system to the user's mobile device, and if so, then packaging the data item in

Art Unit: 2153

an electronic envelope and transmitting the electronic envelope to the user's mobile device (pp. 10-11, describing the messaging system and the filtering of messages at the redirector host system, see also pp. 25-26, 35).

AirMobile further discloses that messages are sent in a "secure and authenticated" manner between the LAN-based server and the mobile wireless device – see p. 25. However, AirMobile does not explicitly state that the secure manner includes encryption. Nonetheless, encryption is a notoriously well-known device used to create secure channels between communicating systems, as evidenced by Liu. In an analogous messaging system, Liu discloses a system where messages are sent to a recipient, wherein the messages are encrypted using private and public keys (Col 13, lines 12-25). The encrypted message is then sent to the recipient device that in turn decrypts the message using a public/private key combination (Col 13, 12-25). The keys for each device are managed using a signature manager on each device (Col 12, lines 55-58). The signature managers communicate keys to a key repository so other devices can access the public keys and also allow for the retrieval of private keys (Col 14, lines 8-24). Given this teaching, a person having ordinary skill in the art would have readily recognized the desirability and advantages of using encryption, as disclosed by Liu, at the mail server, in the system taught by AirMobile to securely transmit messages, because encryption is a very effective way to ensure that messages remain secure throughout their transmission. Therefore, it would have been obvious to encrypt the messages at the AirMobile Wireless for cc:Mail Server in the system taught by AirMobile.

AirMobile and Liu disclosed the invention substantially as claimed however, AirMobile and Liu both failed to specifically recite using the redirector host system to automatically encrypt data items. Nonetheless it was widely known in the art at the time of the invention to

Art Unit: 2153

automatically encrypt data items at redirection servers, as evidenced by Gehrman. In an analogous messaging system Gehrman disclosed a system for redirecting messages from a mail server to user's wireless device (see inter alia Figure 1 and pg 5, lines 12-21; forwarding message from the mail server 24 to the client PC or PDA over wireless connection 20). Further when Gehrman's system determines that a new data item should be redirected (i.e. "meeting the user's predetermined mail forwarding policy) the system automatically encrypts the data item before redirecting it to the client's PDA (see inter alia pg 8, line 29 – pg 9, line 9). Gehrman's system employs this automatic encryption scheme to ensure that unencrypted messages that are going to be sent over unsecured communication networks are first encrypted to ensure messages remain secure throughout their transmission (pg 3, lines 13-26). Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the automatic encryption scheme used by Gehrman's in the combined AirMobile and Liu system to ensure messages remain secure throughout their transmission (pg 3, lines 13-26).

Claims 140-146 and 148-174 are rejected using a similar rationale as applied to claims 105-111 and 113-139.

3. Claim 112 is rejected under 35 U.S.C. 103(a) as being unpatentable over AirMobile, in view of Doonan and Gehrman, and further in view of RFC 2193 (IMAP4 Mailbox Referrals, September 1997).

Art Unit: 2153

4. **Claim 147 is rejected under 35 U.S.C. 103(a) as being unpatentable over AirMobile, in view of Liu and Gehrmann, and further in view of RFC 2193 (IMAP4 Mailbox Referrals, September 1997).**

In considering claims 112 and 147, Doonan and Liu further disclose the use of SSL for the communications (i.e. "https"). However, neither AirMobile nor Doonan nor Liu explicitly disclose the use of IMAP for forwarding the messages. Nonetheless, Doonan and Liu disclose using the Internet and AirMobile discloses forwarding e-mail, and the IMAP protocol is a well known protocol for forwarding e-mail over the Internet, as evidenced by RFC 2193. Thus, given that IMAP is a widely-used protocol for Internet-based e-mail, it would have been obvious to use it in the combined system of AirMobile and Doonan or AirMobile and Liu to avoid the need to create an entirely new protocol.

Response to Arguments

Applicant's arguments are noted however they are moot in view of the new grounds of rejection set forth.

Conclusion

The prior art made of record, in PTO-892 form, and not relied upon is considered pertinent to applicant's disclosure.

THIS ACTION IS MADE NON-FINAL.


Art Unit: 2153

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sean Reilly whose telephone number is 571-272-4228. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glen Burgess can be reached on 571-272-3949. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

March 23, 2006


KRISNA LIM
PRIMARY EXAMINER